UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,854	08/30/2000	Douglas B Moran	RECOP013	2198

21912 7590 05/12/2004

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	PAPER NUMBER
2134	10

DATE MAILED: 05/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/651,854	**Applicant(s)** MORAN, DOUGLAS B	
	Examiner Matthew Heneghan	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 August 2000 and 16 November 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 August 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5,7*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 have been examined.

Priority

The following is a quotation of the appropriate part of 35 U.S.C. 120:

> An application for patent for an invention disclosed in the manner provided by the first paragraph of section 112 of this title in an application previously filed in the United States, or as provided by section 363 of this title, which is filed by an inventor or inventors named in the previously filed application shall have the same effect, as to such invention, as though filed on the date of the prior application, if filed before the patenting or abandonment of or termination of proceedings on the first application or on an application similarly entitled to the benefit of the filing date of the first application and if it contains or is amended to contain a specific reference to the earlier filed application.

2. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 120 as follows: the application to which the instant application has been filed as a continuation, U.S. Patent Application No. 09/615,967, filed 14 July 2000, has no inventors in common with the instant application.

3. The instant application claims priority to Provisional U.S. Patent Application No. 60/151,531, filed 30 August 1999.

Information Disclosure Statement

4. The following Information Disclosure Statement in the instant application has been fully considered:

Paper No. 5, filed 27 December 2000.

Paper No. 7, filed 16 April 2001.

5. Three additional documents have been found in the file wrapper that were not listed on the Form PTO-1449:

Lunt, et al., "Automated Audit Trail Analysis and Intrusion Detection: A Survey, " October, 1988.

Farmer et al., "The COPS Security Checker System," 1990.

Porras et al., "EMERALD : Event Monitoring Enabling Responses to Anomalous Live Disturbances," date unknown.

Each has been fully considered.

Specification

6. The disclosure is objected to because of the following informalities: On page 16, line 9, a reference is incorrectly made to co-pending application 09/615,697. It is presumed that the reference is to 09/615,967.

Appropriate correction is required.

7. The use of the trademarks UNIX® and Solaris® have been noted in this application. They should be capitalized wherever they appear and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Drawings

8. The drawings are objected to under 37 CFR 1.74 and 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, reference numbers for the claimed features, as depicted in Figure 8, must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

9. The drawings are objected to as failing to comply with 37 CFR 1.84(l) because the lines in Figure 2 are not uniformly thick and well-defined. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claim 12 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. There are no files in the claimed environment that can only be accessed by the user account. All such files can also be accessed by a super-user. In the examining of the claims, it will be presumed that any file accessible by only the user and super-user would apply.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 7-12, 19, and 20 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are:

Regarding claim 8, there is no limitation showing how the directory scanner is associated with the other components.

Regarding claim 19, there is no limitation showing how the time delay function is used in the analysis engine.

Claims 8-12 and 20 depend from rejected claims 7 and 19, and include all the limitations of those claims, thereby rendering those dependent claims incomplete.

12. Claims 23 and 24 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are:

No limitation exists that teaches as to how the analysis engine and the discovering step achieve the detection of intrusions.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

13. Claims 1-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Though the specification teaches to the claimed inventions being executed on a computer, the claimed material is solely dedicated to computer programs that simply manipulate abstract information on the computer and which are not tangibly embodied.

14. Claim 24 is rejected under 35 U.S.C. 101 because the claimed recitation of a use, without setting forth clear steps involved in the process, as described above, results in an improper definition of a process, i.e., results in a claim which is not a proper process claim under 35 U.S.C. 101. See for example *Ex parte Dunki*, 153 USPQ 678 (Bd.App. 1967) and *Clinical Products, Ltd.* v. *Brenner*, 255 F. Supp. 131, 149 USPQ 475 (D.D.C. 1966).

15. To expedite a complete examination of the instant application, the claims rejected under 35 U.S.C. 101 and 35 U.S.C. 112 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical

Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

16. Claims 1, 2, 4, 6, and 14-17 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S Patent No. 6,347,374 to Drake et al.

As per claims 1, 2, 4, and 6, Drake discloses an event detection system wherein monitoring is done over a distributed environment (where the monitor may be apart from the host), and files containing system file locations, such as the Windows NT registry are referenced (see column 18, line 49 to column 19, line 5). Drake discloses that this information is used to detect login attempts, so the login files must inherently have been retrieved in the process (see column 15, lines 29-67).

As per claims 14-16, the system disclosed by Drake collects all the files relevant to an audit from a host's directory and tailors the process to each target system according to a specified collection sequence (see column 9, line 38 to column 10, line 32).

As per claim 17, Drake does not specify a limit as to the elapsed period of the logfiles. The only prerequisite to being able to collect a year's worth of data in such a system is the ability to measure in terms of years, and this functionality is supported in Drake (see column 7, line 5).

17. Claims 1-3, 7, 19, 20, 23, and 24 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S Patent No. 6,405,318 to Rowland.

As per claims 1-3 and 7, Rowland discloses the analysis of wtmp and utmp records, as well as user time records (see column 4, lines 30-57).

As per claims 19 and 20, Rowland discloses the collecting of log information on a host in a user profile database (see column 4, lines 48-61) and checks that database to determine anomalies in view of the time that a user has logged in (see column 5, lines 20-30), as is done in the time decay function. The day and time of a login is compared to that profile, it order to determine if it is suspicious.

As per claims 23 and 24, Rowland analyzes the content of system files for detecting intrusion (see claim 8, item (a)(ii)).

18. Claims 7 and 8 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,485,409 to Gupta et al.

Gupta discloses intrusion detection based upon at least three sets of information (see column 6, lines 12-20), and analyzes inode information (see column 37, line 55 to column 38, line 9).

Claim Rejections - 35 USC § 103

19. Claims 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,405,318 to Rowland as applied to claim 2 above, and further in view of Frisch, "Essential System Administration," 1995, pp. 264-265.

Regarding claims 4 and 5, Rowland discloses the retrieval of certain system configuration files, but does not disclose that they can be found by referencing syslog.conf.

Frisch discloses that syslog.conf designates the locations of the files for storing system messages.

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made modify the invention of Rowland by retrieving the system configuration files using syslog.conf, as disclosed by Frisch, since it contains the locations of some system files.

20. Claims 8-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,405,318 to Rowland as applied to claim 7 above, and further in view of U.S. Patent No. 5,485,409 to Gupta et al.

Regarding claim 8, Rowland does not refer to the specific analysis of i-nodes.

Gupta discloses the analysis of inodes for intrusion detection, as described above, and further suggests that this is because policies may exist where write-access to an inode is required.

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made modify the invention of Rowland by analyzing I-nodes, as disclosed by Gupta, as because policies may exist where write-access to an inode is required.

As per claims 9 and 10, Rowland discloses information being collected on wtmp, another file (utmp), with access time information (see column 4, lines 30-47).

21. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,405,318 to Rowland in view of U.S. Patent No. 5,485,409 to Gupta et al. as applied to claim 10 above, and further in view of Frisch, "Essential System Administration," 1995, pp. 262-263.

Rowland and Gupta do not specifically disclose the checking of sulog for information.

Frisch discloses the logging of information pertaining to uses to the su command in sulog, and further suggests that repeated unsuccessful login attempts from any user account can indicate someone trying to break in to the system.

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made modify the invention of Rowland and Gupta by monitoring sulog, as disclosed by Frisch, since repeated unsuccessful login attempts from any user account can indicate someone trying to break in to the system.

22. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,405,318 to Rowland in view of U.S. Patent No. 5,485,409 to Gupta et al.

as applied to claim 9 above, and further in view of U.S. Patent No. 6,453,345 to Trcka et al.

Rowland and Gupta do not disclose the collection of information of timestamps relating to directories and files.

Trcka discloses the adding of timestamps to the data stream relating to file usage in order to record proof of user misconduct.

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Rowland and Gupta by collecting timestamps with respect to file usage, as disclosed by Trcka, in order to record proof of user misconduct.

Since this data would be collected for all files, this would include those only accessible to the user account.

23. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,485,409 to Gupta et al. as applied to claim 8 above, and further in view of U.S. Patent No. 6,453,419 to Flint et al.

Gupta does not disclose the checking of log files for null-bytes.

Flint discloses the checking for NULL entries in a file, so that memory can be freed (see column 8, lines 39-43).

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Gupta to check files for null-bytes, as disclosed by Flint, in order to free up memory.

24. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,347,374 to Drake et al. as applied to claim 17 above, and further in view of Frisch, "Essential System Administration," 1995, p.250.

Drake discloses the retrieval of appropriate files from a system, but does not specify that log files are stored in "syslog."

Frisch discloses that syslog.conf is an important file to protect and monitor in UNIX®.

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Drake by retrieving a syslog file, such as syslog.conf, from a UNIX® system, as disclosed by Frisch, since it is an important file to protect and monitor.

Allowable Subject Matter

25. Claims 21 and 22 would be allowable if rewritten to overcome the rejection under 35 U.S.C. 101, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

26. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claim 21, no art could be found that would compute the probability for the end of a session in the context of intrusion detection. The closest art, U.S. Patent No. 6,278,966 to Howard, does employ calculations of session end probability (see column 9, lines 28-33), but does so as part of a simulation intended to predict the impact of a change to a configuration on the overall system performance. No motivation exists for using this probability, as disclosed by Howard, to compute a suspicion value.

Claim 22 would be allowable due to the fact that it is dependent upon base claim 21. Regarding the claim itself, the auditing of an su session is disclosed in U.S. Patent No. 5,032,979 to Hecht, and Frisch discloses the storing of su information in sulog, as described above.

Conclusion

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,557,742 to Smaha et al. discloses a system for collecting and analyzing audit logs.

U.S. Patent No. 5,991,881 to Conklin et al. discloses a system for network surveillance using logs.

U.S. Patent No. 6,681,331 to Munson et al. discloses a system for detecting intrusions via statistical analysis.

28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH

May 5, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100